IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF:	
DEVICES A-E	Magistrate No. 23-46 **[UNDER SEAL]**
DEVICES F-J	Magistrate No. 23-47 **[UNDER SEAL]**
DEVICES K-O	Magistrate No. 23-48 **[UNDER SEAL]**
DEVICES P-T	Magistrate No. 23-49 **[UNDER SEAL]**
DEVICES U-Y	Magistrate No. 23-50 **[UNDER SEAL]**
DEVICES Z-DD	Magistrate No. 23-51 **[UNDER SEAL]**
DEVICES EE-II	Magistrate No. 23-52 **[UNDER SEAL]**
DEVICES JJ-NN	Magistrate No. 23-53 **[UNDER SEAL]**
DEVICES OO-SS SEIZED FROM 5134 MCROBERTS RD, PITTSBURGH, PA 15234 AND	Magistrate No. 23-54 **[UNDER SEAL]**
DEVICES TT-VV SEIZED FROM 5332 ELMWOOD DR, PITTSBURGH, PA 15227 AND CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION SECURE EVIDENCE ROOM 3311 EAST CARSON ST PITTSBURGH, PA 15203	Magistrate No. 23-55 **[UNDER SEAL]**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Lauren Scott, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose, and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Your Affiant makes this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices, as described in Attachment A—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am employed as a Special Agent of the Federal Bureau of Investigation and have been so employed since December 2020. I am currently assigned to the Pittsburgh Division of the FBI, working Violent Crimes Against Children Matters. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. In addition to my training, I have participated in the execution of numerous search warrants related to computer crimes, the majority of which have involved child exploitation and/or child sexual assault material. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The statements contained in this Affidavit are based upon my investigation, information provided by other sworn law enforcement officers and witnesses, other personnel specially trained in the seizure and analysis of computers and electronic mobile devices and

electronic storage devices, and on my experience and training as a federal agent.

4. This Affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the information set forth in this Affidavit, there is probable cause to believe that on the electronic devices specifically described below and in Attachment A (hereinafter collectively referred to as the "**TARGET DEVICES**") there exists fruits, instrumentalities, contraband, and evidence of violations of Title 18, United States Code, Section 2252(a), which makes it a crime to transport, receive, distribute, and possess material depicting the sexual exploitation of a minor (child pornography). I am requesting authority to search the entirety of the **TARGET DEVICES**, for the items specified in Attachment B, hereto, which items constitute fruits, instrumentalities, contraband, and evidence of the foregoing violations. The **TARGET DEVICES** are specifically described in Attachment A.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

6. The property to be searched (the **TARGET DEVICES**) was seized from 5134 McRoberts Rd, Pittsburgh, PA 15234 ("a" through "ss") and 5332 Elmwood Drive, Pittsburgh, PA 15227 ("tt" through "vv") by Allegheny County Adult Probation Officers on August 16, 2022 and is described as follows:

a. One (1) HP Laptop Model Number 15-BS113DX, S/N# CND8131Q4Q

b. One (1) SanDisk Cruzer Blade – BM180426374B – 32GB

c. One (1) SanDisk Micro SD – 128GB – 9531YX0HV5WS

d. One (1) Samsung 128D Micro SD – DCQGX36GQ635

e. Three (3) SanDisk Cruzer Blade 32GB – BM170625684B

f. One (1) SanDisk Cruzer Blade 32GB – BM1804 (the rest being scratched off), Pink

g. Two (2) SanDisk Cruzer Blade 32GB – BM170325721B

h. One (1) SanDisk Cruzer Blade 32GB – BM180426374B

i. One (1) SanDisk Cruzer Dial 64GB – BN170425469B

j. One (1) SanDisk Cruzer Glide 32GB – BM150325242B

k. One (1) SanDisk Cruzer Glide 128GB – BP180426551B

l. One (1) SanDisk Ultra USB 64GB - BN160725619B

m. Two (2) SanDisk Ultra USB 128GB – BP180525364B

n. One (1) SanDisk Ultra USB 128GB – BP180826263B

o. One (1) SanDisk Ultra USB 128GB – BP200158179W

p. One (1) SanDisk Ultra USB 128GB – BP180725783B

q. One (1) SanDisk Ultra USB 128GB – BP200157396W

r. One (1) SanDisk Ultra USB 256GB – BQ181125916B

s. One (1) SanDisk Ultra USB 256GB – BQ180626269B

t. One (1) SanDisk 8GB USB – BI1111ZKTD

u. One (1) SanDisk 8GB USB – BI130824570V

v. One (1) SanDisk SD 512 MB – AX0624104182B

w. One (1) SanDisk SD 512 MB – AX0711511397D

x. One (1) Kodak SD 512 MB – 50110637L066

y. One (1) SanDisk Ultra II SD 1GB – B130631605228D

z. One (1) SanDisk MicroSD 128GB – 9093DVEXX0FO

aa. One (1) SanDisk MicroSD 128GB – 9531YXOHV1XA

bb. One (1) SanDisk MicroSD 128GB – 0023YXCYF2R2

cc. One (1) SanDisk MicroSD 128GB – 2123OC764584

dd. One (1) SanDisk MicroSD 256GB – 2093YCEKV14X

ee. One (1) SanDisk MicroSD 256GB – 8275DVCHQ06C

ff. One (1) SanDisk MicroSD 200GB – 8475DVKX80RY

gg. One (1) SanDisk MicroSD 32GB – 8166ZVAHR4X2

hh. One (1) SanDisk MicroSD 64GB – 8104DPLAK0QG

ii. One (1) Samsung Micro SD 128GB – DCQDH50GD636

jj. Two (2) Samsung Micro SD 128GB – DCQGX36GU635

kk. Two (2) Samsung Micro SD 128GB – DCQD1B1GK627

ll. One (1) Samsung Micro SD 128GB – DCQDK00GY635

mm. One (1) SanDisk Ultra USB 128GB – BP180726263B

nn. One (1) SanDisk Ultra USB 256GB – BQ180926263B

oo. One (1) SanDisk CruzerBlade 32 GB – BM70926126B

pp. One (1) SanDisk USB 32GB – BM170525476V

qq. One (1) Kingston Data Traveler 2GB – CH051008

rr. One (1) Blue USB – Entertainment Unlimited 8GB

ss. One (1) Orange USB Particle Measuring Systems

tt. One (1) San Disk SD Card 1GB – BB0814813316B

uu. One (1) Casio Exilim – 7125105A

vv. One (1) GoPro Hero 5, FCCID: CNFHWM91

7. The **TARGET DEVICES** are currently located in the Secure Evidence Room at The Federal Bureau of Investigation, 3311 East Carson St, Pittsburgh, PA 15203.

8. The applied-for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying the electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. On September 27, 2018, James WRIGHT (DOB: XX/XX/1977),[1] was sentenced to a total term of five (5) years' probation after pleading guilty to child exploitation offenses in the Allegheny County Court of Common Pleas, Commonwealth of Pennsylvania. Specifically, at Criminal Case No. CP-02-CR-0013321-2017, WRIGHT pleaded guilty on July 11, 2018 and was sentenced on four (4) counts: (1) Unlawful Contact With Minor – Sexual Offenses (F3), in violation of 18 Pa. C.S. § 6318(A)(1); (2) Corruption of Minors (M1), in violation of 18 Pa. C.S. § 6301(A)(1)(i); (3) Indecent Assault Person Unconscious (M1), in violation of 18 Pa. C.S. § 3216(A)(4); and (4) Indecent Exposure (M1), in violation of 18 Pa. C.S. § 3127(A).[2] WRIGHT'S convictions stem from his criminal conduct at Kennywood Park (an amusement park in the Western District of Pennsylvania) in 2017. According to the Criminal Complaint filed by the West Mifflin Police Department, on July 31, 2017, WRIGHT (who was later identified through Kennywood's video surveillance footage) followed two minor female victims (12 and 13 years old) while in the park. The minors reported that WRIGHT kept getting very close to them (as they tried to distance themselves from him) while waiting in line for a ride. One of the minors reported that when WRIGHT was close to her, she felt "something warm" go

[1] WRIGHT's exact date of birth is known to your Affiant and provided with only the year here pursuant to Local Rule of Criminal Procedure 5.2(D)(3).

[2] The publicly available case docket also indicates that WRIGHT pleaded guilty to a fifth count - Open Lewdness (M3), in violation of 18 Pa. C.S. § 5901; however, it does not appear that WRIGHT was sentenced on this count.
See https://ujsportal.pacourts.us/Report/CpCourtSummary?docketNumber=CP-02-CR-0013321-2017&dnh=8I22pUMofQoFsWt5aM9q3Q%3D%3D (last visited January 10, 2023).

onto her left leg, then observed liquid on her leg, sock, and shoe, and saw that WRIGHT's penis was exposed outside of his shorts. The minor confronted WRIGHT who kept repeating: "I'm sorry, I have a problem." The minors later reviewed Kennywood video surveillance and identified WRIGHT. On the surveillance footage, law enforcement further observed that, on multiple occasions, WRIGHT appeared to take video/pictures of other underage females in the park. When viewing the surveillance video, law enforcement also observed WRIGHT following groups of young girls.

10. WRIGHT is currently under Allegheny County Adult Probation Supervision (ACPS) and Sex Offense Court Supervision until September 27, 2023. This means that, in addition to the general rules and conditions of probation routinely imposed by Allegheny County's Fifth Judicial District, WRIGHT'S probation conditions include charge-specific conditions. For example, WRIGHT is "not to have contact with children under the age of 18 (beyond incidental contact or in the presence of an adult who has been approved by his Probation Officer and is aware of the nature of WRIGHT'S offense)." The court also authorized the Allegheny County Adult Probation Office to conduct periodic, unannounced examinations of WRIGHT'S computer equipment. (WRIGHT'S conditions and special conditions of probation are attached hereto as Exhibits 1 and 2, respectively). Further, because of the nature of his conviction, WRIGHT must register as a sex offender while residing, living, or working within the state of Pennsylvania for 25 years from the date of his conviction (Megan's Law Offender - Tier 2).[3]

[3] Your Affiant notes that County Probation also informed that, while on probation, WRIGHT has traveled out of state on numerous occasions, attended multiple events throughout the state of Pennsylvania, including holiday parades and concerts, where WRIGHT filmed adult and minor females in various positions, as to show their buttocks in close range of the camera. County Probation believes that none of these individuals had knowledge of WRIGHT's filming.

11. In August 2022, the Baldwin Police Department (Pennsylvania) received information from law enforcement in Alexandria, Virginia concerning WRIGHT filming patrons at a water park. Specifically, on August 16, 2022, Alexandria City Police Department officers responded to the Great Waves Waterpark, located 4001 Eisenhower Avenue, Alexandria, VA 22304, because Waterpark staff and multiple patrons reported observing an adult male utilizing a GoPro camera to film patrons of the Waterpark while under water. Alexandria City Police Officers identified WRIGHT as the male filming families under the water. Officers then spoke with WRIGHT who admitted to having a GoPro in his possession but claimed it was inoperable. Upon identifying WRIGHT, Alexandria City Police Officers learned that WRIGHT is an active registered sex offender in the State of Pennsylvania under Megan's Law and notified the Baldwin Police.[4] WRIGHT was escorted out of and banned from the park on the same date. As WRIGHT was escorted from the water park, law enforcement officers obtained WRIGHT'S vehicle information – a 2018 Silver Hyundai Santa Fe with license plate number GCN-4347.

12. Because WRIGHT's probation conditions prohibited him from traveling outside of the state of Pennsylvania without written permission, Officers with the Allegheny County Adult Probation Department (hereinafter "County Probation") contacted WRIGHT's sentencing judge, the Honorable Jill E. Rangos, who directed, via email, on August 19, 2022 County Probation Officers to detain WRIGHT for technical violations of his probation conditions.[5]

---

[4] WRIGHT previously had reported to the Allegheny County Adult Probation Department that he resided at 5332 Elmwood, Pittsburgh, PA 15227, and he had registered as a sex offender pursuant to PA's Megan's Law at this address, which is located within Baldwin Borough, Pennsylvania.

[5] In addition to failing to seek permission to travel and report that he did, in fact, travel outside of the Commonwealth of Pennsylvania, County Probation Officers contacted Judge Rangos because WRIGHT did not report his contact with the Alexandria City Police Department to County

Judge Rangos also authorized a search of WRIGHT's reported residence at 5332 Elmwood, Pittsburgh, PA 15227 (Baldwin). However, when Probation Officers visited WRIGHT's Baldwin residence, he was not home. WRIGHT'S mother (also a resident at this address) informed County Probation Officers that WRIGHT had left the residence to set up for a work event. When a Probation Officer called WRIGHT via phone, he confirmed the same. Thus, Probation Officers began looking for WRIGHT.

13. In their search for WRIGHT, Probation Officers reviewed WRIGHT'S supervision history and learned that WRIGHT had reported to his previous Probation Officer that he was the caretaker of a residence owned by a relative and located at 5134 McRoberts Rd, Pittsburgh, PA 15234 (although this location was not WRIGHT's reported residence to County Probation). County Probation Officers learned, via an open-source query, that the owner of the residence currently resides in Largo, Florida, and has for the last several years. Upon receiving this information, County Probation Officers believed that WRIGHT could be staying at the McRoberts residence, which was unauthorized. Therefore, County Probation Officers began to surveille both addresses (WRIGHT'S reported residence at 5332 Elmwood Drive, Pittsburgh, PA 15227 and the residence for which he previously reported being a caretaker - 5134 McRoberts Road, Pittsburgh, PA 15234) for WRIGHT and his known vehicle (a 2018 Hyundai Santa Fe with license plate number GCN-4347).

14. County Probation Officers subsequently observed WRIGHT's vehicle parked at 5134 McRoberts Road, Pittsburgh, PA 15234 at various times on August 19, 21, and 23, 2022, and at 5332 Elmwood, Pittsburgh, PA 15227, on August 20 and 21, 2022. On August 23, 2022,

---

Probation, and Officers were concerned about WRIGHT having possibly had contact with a minor and his possession of a GoPro camera, given that his prior conviction was similar in nature to the conduct alleged in Alexandria, Virginia.

PA Probation Officers observed WRIGHT physically present at the residence at 5134 McRoberts Rd, Pittsburgh, PA 15234—a County Probation Officer unknown to WRIGHT knocked on the front door of the residence; WRIGHT answered after several minutes and apologized for the time it took him to come to the door, stating that he was "down in the basement". Based on these observations, County Probation now believed that WRIGHT was likely utilizing the residence at 5134 McRoberts Road for purposes other than "caretaker", in violation of his probation conditions,[6] and made plans to detain WRIGHT and search the residence for any contraband relating to WRIGHT's probation violations and to verify compliance with all conditions of supervision.

15. On August 29, 2022, County Probation Officers observed WRIGHT'S vehicle parked in the driveway of the residence of 5134 McRoberts Road and knocked on the door. WRIGHT answered the door but identified himself as "Jimmy". WRIGHT was identified by other County Probation Officers familiar with him. At that time, WRIGHT was detained and a walk through of the residence conducted. Upon entering the residence, County Probation Officers observed the following in plain view:

a. a wallet with a driver's license belonging to WRIGHT – on the dining room table, first floor

b. several "Ziploc" bags containing various memory devices (i.e., SD cards, Flash drives); some of these devices were located within "Altoids" brand containers, which were lined with tin foil – on top of the couch, living room

c. a laptop charging cable (found plugged into an outlet) – living room

[6] WRIGHT did not report this as an address of residency to County Probation and had not registered the address under Megan's Law.

d. a gold Samsung smart phone – on a tv stand, living room

e. various forms of medical marijuana – on tv stand/in drawer, living room

16. Noting WRIGHT'S violation of the General Rules and Special Conditions of Probation (e.g., Condition 8 – no travel outside of Pennsylvania is permitted and Condition 16 – Requiring Compliance with Court-Imposed Special Conditions, *see* Exhibit 2), County Probation Officers then conducted a search of the residence to ensure that no further contraband existed. During the search, the following was located:

a. various forms and amounts of liquor – from cabinet in kitchen, first floor

b. two "flip phones" - one from the kitchen; one from a duffel bag in living room

c. "White Claw" alcoholic seltzer water – from refrigerator in kitchen, first floor

d. various digital and analog cameras – in office, first floor

e. an HP laptop with a pink flash drive with a red/black SanDisk MicroSD Card plugged into it – underneath the couch in the living room, first floor

f. various Disney DVDs – inside of a cardboard box and grocery bags in the living room, first floor

g. indicia for WRIGHT in the form of a purchase order from May 2021 for "Jessie 2011 The Complete Series on DVD Cameron Boyce Debby Ryan Peyton List Disney Nickelodeon" with "FANMADEDVD" shipped to James Wright, 5332 Elmwood Dr, Pittsburgh, PA 15227 – inside of a cardboard box and grocery bags in the living room, first floor

17. County Probation Officers questioned WRIGHT regarding his possession of the

devices and his unauthorized travel from the state of Pennsylvania. WRIGHT admitted to traveling from the state of Pennsylvania to the state of Virginia on August 16, 2022 and, later that day, to Washington D.C. WRIGHT further admitted that he did not receive prior approval from County Probation to leave the state of Pennsylvania, stating that he believed he only had to do so if it was for "longer than 10 days". WRIGHT admitted to going to the waterpark on the same date and stated he used his GoPro camera to film himself inside the park while he was on the waterslide.

18. During questioning concerning his presence at the home on McRoberts Road, WRIGHT stated he is the caretaker for the house, and reported the house belongs to "Aunt Debbie". WRIGHT stated he "squats" at the residence and is between the McRoberts home, his parents' home (meaning the Elmwood residence), and his girlfriends' home. WRIGHT claimed the Samsung Smart Phone is his dad's old phone; that it was not functioning/in use; and denied utilizing it. WRIGHT stated the memory devices were his; however, he claimed they all had "music" on them. WRIGHT said the HP laptop was his, and that he had it prior to starting his current term of county probation. [Note: Probation Officers opened this laptop on site and observed that "James Wright" is the labeled user profile for the device, with no other profiles on the device. WRIGHT refused to provide the password for the laptop. Upon discovery of the laptop, WRIGHT spontaneously uttered: "f***".] When questioned about the GoPro device, WRIGHT stated the device was presently at his parents' home and that an additional digital camera would be present at the residence of 5332 Elmwood, Pittsburgh, PA 15227 (WRIGHT'S parents' home). WRIGHT gave County Probation Officers verbal consent to retrieve these items.

19. WRIGHT was taken into custody by the Allegheny County Sheriff's Department

and lodged at Allegheny County Jail on a County Probation detainer, where he currently remains. Once WRIGHT was in custody, County Probation Officers went to the residence of Richard and Kathleen Wright (WRIGHT'S parents) at 5332 Elmwood, Pittsburgh, PA 15227 (WRIGHT's reported address of residency to County Probation). K. Wright gave Probation Officers verbal consent to search the residence and then directed Officers to WRIGHT's room. Officers seized the following contraband: A black GoPro, a silver digital camera, and various medical marijuana.

20. WRIGHT remains incarcerated for several technical violations of his conditions of county probation: leaving the state of Pennsylvania without permission, failure to comply with special order of the court (setting special conditions of probation, *see* Exhibit 2), being a danger to self and/or others, and failure to be of good behavior.

21. The following devices were seized from the residence located at 5134 McRoberts Rd, Pittsburgh, PA 15234 (the residence where Probation Officers located WRIGHT):

a. black HP Laptop (in "airplane mode"), with charging cable – under living room couch, plugged into power outlet in living room

b. black SanDisk MicroSD Card Adapter with SanDisk 128 GB MicroSD card inserted – plugged into HP laptop

c. pink SanDisk Cruzer Blade 32 GB Flash Drive - plugged into the HP Laptop

d. white USPS Mail Bag containing nine various Disney DVDs and paper indicia for James Wright from May 5, 2021 (described above at paragraph 16, subsections f and g) – on couch in living room

e. gold Samsung Galaxy S7 SM-G30P IMEI 358991076020732 – on tv stand

in living room

f. plastic bag containing numerous memory devices, some contained in green Altoid cans, lined with foil – from couch in living room

g. black "Sonim" Model flip phone – in bag on dining room table

h. black "Kyocera" Model flip phone – in bag on dining room table

i. various medical marijuana, in various forms – on/inside tv stand in living room

j. silver Canon AE-1 film camera with brown leather case and multi-colored strap – in closet in side bedroom

k. black Model Freedom Zoom 70C E5 Camera SN#36210755

l. silver/Black Model Pocket Everflash 120 Keystone Camera with Leather "Keystone" carrying case

m. black Sony Cyber-Shot G Digital Camera with carrying case

22. The following devices were seized from WRIGHT'S bedroom at his parents' residence located at 5332 Elmwood Dr, Pittsburgh, PA 15527:

a. black GoPro Hero 5 Session Action Camera with Black Mount and Charging Cable

b. silver Casio Exilim Camera with SD card

c. various medical marijuana in various forms

23. County Probation Officers previewed several of the memory devices seized (from those listed above) and observed child sexual abuse material (i.e., child pornography). Probation Officers then contacted your Affiant who observed the same. For example, Probation Officers observed: a video of a prepubescent female dancing and exposing her vagina; multiple pictures

of prepubescent females exposing their vaginas in various poses; and homemade videos in which WRIGHT is believed to be walking around stores, obtaining "close-ups" of women of all ages. On one of the non-encrypted memory devices[7], a video was located of WRIGHT appearing to babysit two girls (Minor Victim 1 (MV1) and Minor Victim 2 (MV2)) who appear to be under the approximately age of 12. This video depicts WRIGHT walking around the residence at 5332 Elmwood, Pittsburgh, PA 15527 with MV1 and MV2, and showing them his room, as well as various other rooms. WRIGHT filmed MV1 and MV2 from behind while they played in the living room. The video captured WRIGHT placing his penis in view of the camera and beginning to masturbate. When MV 1 or MV2 turned around, WRIGHT took his penis out of view of the camera. WRIGHT did this on multiple occasions during the video. On one such occasion, after putting his penis in view of the camera, WRIGHT touched the hair of one of the minor victims; the minor victim did not seem to react. The minor victims had their backs to WRIGHT when his penis was exposed. The minors were fully clothed in the video.

24. Your Affiant further notes another known incident involving WRIGHT and minors that occurred on July 30, 2019. On this date, Officers of the University of Pittsburgh Police Department were working the JoJo Siwa concert at the Peterson Events Center and received a complaint that a male was following a mother and daughter around. When the male was approached by law enforcement, he stated he did not possess any ID card and provided Officers with the name J.T. Doman of Youngstown, Ohio, with DOB 2/20/1998. The individual confirmed that "J.T." stood for "John Thomas". Officers ran the information ran through

[7] In previewing WRIGHT'S devices, County Probation Officer and your Affiant viewed the video described herein. This memory device is included within the memory devices seized from WRIGHT and sought to be searched as part of this warrant. *See* paragraph 6. At this time, neither your Affiant nor County Probation Officers recall which of the numerous devices listed herein contained the observed CSAM.

dispatch with negative results. After numerous attempts to obtain accurate information with no result, the male was detained. At that time, the male identified himself as James Richard Wright, DOB XX/XX/1977. WRIGHT then confirmed he was a registered sex offender.

25. Based on all of the above, your Affiant requests a search warrant to review the **TARGET DEVICES** for evidence of violations of Title 18, United States Code, Section 2252 (transportation, distribution, receipt, possession of material depicting a minor engaged in sexually explicit conduct (child sexual abuse material – i.e., child pornography)).

DEFINITIONS

26. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "Minor," as defined in 18 U.S.C. § 2256(1), means any person under the age of 18 years.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child Pornography," or "Child Sexual Abuse Material," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been

created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in "sexually explicit conduct," as that term is defined in 18 U.S.C. § 2256(2). Herein, material constituting child pornography is also called "child sexual abuse material" or "CSAM".

d. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

f. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone

number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

g. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

h. "Digital camera": A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include

a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

i. "Internet Service Providers" or "ISPs," are businesses that enable individuals to obtain access to the Internet. ISPs provide their customers with access to the Internet using telephone or other telecommunications lines, provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers, remotely store electronic files on their customers' behalf, and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, electronic mail transaction information, posting information, account application information, and other information both in computer data and written format.

j. An "Internet Protocol" or "IP" address is a unique numeric address used by computers or cellular telephones on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer connected to the Internet must have an assigned IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a particular range of IP addresses. When a customer connects to the Internet using an ISP service, the ISP assigns the

computer an IP address. Any and all computers using the same ISP account during that session will share an IP address. The customer's computer retains the IP address for the duration of the Internet session until the user disconnects. The IP address cannot be assigned to a user with a different ISP account during that session. When an Internet user visits any website, that website receives a request for information from that customer's assigned IP address and sends the data to that IP address, thus giving the Internet user access to the website.

k. "Internet": The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

l. "Storage medium," as used herein, is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

27. Based on my training, experience, and research, I know that a cellular telephone has capabilities that allow it to serve as a wireless telephone, computer, digital camera, and portable media player. Laptop computers, desktop computers, and hard drives, allow for the storage of large amounts data, including Internet browsing histories, documents, images, and videos. They also function as a repository for backing up data from cellular telephones, namely images and video files. In my training and experience, examining data stored on devices of this

type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

28. In my training and experience, I know that computers and electronic mobile devices essentially serve four functions in connection with child pornography: (1) production; (2) communication; (3) receipt/distribution; and (4) storage.

29. Child pornographers can now easily transfer existing hard copy photographs into a computer-readable format with a scanner. With the advent of digital cameras, images can be transferred directly from the digital camera onto an electronic mobile device or a computer. Moreover, a device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

30. The Internet affords collectors of child pornography several different venues for obtaining viewing and distributing child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by internet portals such as Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or devices with access to the Internet. Evidence of such online storage of child pornography is often found in the user's computer.

31. A computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly

referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

32. With the advent of smart phones and advanced technology, cellular telephones and other electronic mobile devices function as "computers" in the sense that they can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. In fact, some cellular telephones are equipped with memory or SIM cards, which are compact removable storage devices commonly used to store images and other electronic data that can be inserted into a telephone's camera as well as other small digital devices such as tablet devices or handheld computers. Much like "thumb drives," some memory cards have the ability to store large amounts of electronic data, including thousands of images or videos, and on occasion entire operating systems or other software programs. Moreover, cellular telephones offer a broad range of capabilities. In addition to enabling voice communications and containing a "call log" that records phone call details, cellular telephones offer the following capabilities: storing names and phone numbers in electronic "address books;" sending receiving, and storing text messages and e-mails; taking, sending, receiving, and storing still photographs and moving videos; storing and laying back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet.

33. Communications made by way of computer or electronic mobile devices can be saved or stored on the items used for these purposes. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or electronic mobile devices, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally. For example, traces of the path of an electronic

communication may be automatically stored in many places like temporary files or Internet Service Provider client software. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer or electronic mobile devices contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

34. Computer and electronic mobile devices users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer and electronic mobile devices users can also attempt to conceal data by using encryption, which means that a password or devices, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer and electronic mobile devices users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." By using steganography, a computer or electronic mobile devices user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

35. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive or other electronic storage media, deleted or viewed via the Internet. Electronic files saved to a hard drive or electronic storage media can be

stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer or electronic mobile devices, the data contained in the file does not actually disappear; rather, that data remains on the hard drive or electronic storage media until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (i.e., space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten).

36. In addition, a computer's (or electronic mobile device's) operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive or electronic storage media depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer or electronic mobile devices habits. A substantial amount of time is necessary to extract and sort through data in this free or unallocated space.

37. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), computers and electronic mobile devices can contain other forms of electronic evidence as well. In particular, records of how a computer or electronic mobile devices has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records,

documents, programs, applications and materials contained on the computer and electronic mobile devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that can be neatly segregated from the hard drive image as a whole. Digital data on the hard drive or electronic storage media not currently associated with any file can provide evidence of a file that was once on the hard drive or electronic storage media but has since been deleted, edited, or deleted in part such as a word processing file with a deleted paragraph. Virtual memory paging systems can leave digital data on the hard drive or electronic storage media that show what tasks and processes on the computer or electronic storage media were recently used. Web browsers, e-mail programs, and chat programs store configuration data on the hard drive or electronic storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer or electronic mobile devices was in use. Computer file systems (or those on electronic mobile devices) can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital devices, or point toward the existence of evidence in other locations.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN AND IMAGES OF CHILDREN

38. Based on my previous investigative experience related to child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who have a sexual interest in children share certain characteristics:

a. Such individuals may receive sexual gratification, stimulation, and

satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, whether in person, in photographs or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs and video (including electronic files), magazines, books, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their child sexual abuse material (child pornography) in the privacy and security of their home, or some other secure location, and typically retain this material for many years. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

d. Likewise, such individuals often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer or electronic mobile device. These collections are often maintained for several years and are kept close by, usually at the individual's residence or, at times, on their person, in their vehicle, or in

cloud-based online storage, to enable the individual to easily view the collection of child sexual abuse depictions, which is valued highly.

e. Some of these individuals also have been found to download, view, and then delete child sexual abuse material (child pornography) on their computers or digital devices in a cyclical and repetitive basis. Importantly, evidence of such activity, including deleted images and videos of child pornography, can often be located on such an individual's computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time, even after the individual has "deleted" it. This is particularly important because while individuals with an interest in the sexual exploitation of children and CSAM (child pornography) often maintain their CSAM for many years and keep it close by, some of these individuals, due to their knowledge of monitoring by law enforcement and ESP/ISPs, have also been found to download, view, and then delete their CSAM on their computers or digital devices on a cyclical and repetitive basis in an attempt to avoid detection and with the knowledge that they can reacquire the CSAM again with the assistance of high-speed broadband internet.

f. Such individuals also may correspond with and/or meet others to share information and materials, and are known to rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material;

and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

39. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **TARGET DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled a device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the devices and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the later examination of the devices

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

42. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

43. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a) may be located in the **TARGET DEVICES** currently located in the Secure Evidence Room at The Federal Bureau of Investigation, 3311 East Carson St, Pittsburgh, PA 15203 (more fully described in Attachment A).

44. The above information is true and correct to the best of my knowledge, information and belief.

45. I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICES** described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

46. It is further respectfully requested that this Court issue an Order sealing, until further order of Court, all papers submitted in support of this Application, including the Application, Affidavit, and the Search Warrant, and the requisite inventory notice. Sealing is

necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact of this continuing investigation and may jeopardize its effectiveness.

/s/ Lauren Scott
Lauren Scott
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 12th day of January, 2023.

THE HONORABLE PATRICIA L. DODGE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched, collectively referred to as the "**TARGET DEVICES**", was seized from 5134 McRoberts Rd, Pittsburgh, PA 15234 ("a" through "ss") and 5332 Elmwood Drive, Pittsburgh, PA 15227 ("tt" through "vv") and is currently located in the Secure Evidence Room at The Federal Bureau of Investigation, 3311 East Carson St, Pittsburgh, PA 15203, and is specifically described as follows:

a. One (1) HP Laptop Model Number 15-BS113DX, S/N# CND8131Q4Q

b. One (1) SanDisk Cruzer Blade – BM180426374B – 32GB

c. One (1) SanDisk Micro SD – 128GB – 9531YX0HV5WS

d. One (1) Samsung 128D Micro SD – DCQGX36GQ635

e. Three (3) SanDisk Cruzer Blade 32GB – BM170625684B

f. One (1) SanDisk Cruzer Blade 32GB – BM1804 (the rest being scratched off), Pink

g. Two (2) SanDisk Cruzer Blade 32GB – BM170325721B

h. One (1) SanDisk Cruzer Blade 32GB – BM180426374B

i. One (1) SanDisk Cruzer Dial 64GB – BN170425469B

j. One (1) SanDisk Cruzer Glide 32GB – BM150325242B

k. One (1) SanDisk Cruzer Glide 128GB – BP180426551B

l. One (1) SanDisk Ultra USB 64GB - BN160725619B

m. Two (2) SanDisk Ultra USB 128GB – BP180525364B

n. One (1) SanDisk Ultra USB 128GB – BP180826263B

o. One (1) SanDisk Ultra USB 128GB – BP200158179W

p. One (1) SanDisk Ultra USB 128GB – BP180725783B

q. One (1) SanDisk Ultra USB 128GB – BP200157396W

r. One (1) SanDisk Ultra USB 256GB – BQ181125916B

s. One (1) SanDisk Ultra USB 256GB – BQ180626269B

t. One (1) SanDisk 8GB USB – BI1111ZKTD

u. One (1) SanDisk 8GB USB – BI130824570V

v. One (1) SanDisk SD 512 MB – AX0624104182B

w. One (1) SanDisk SD 512 MB – AX0711511397D

x. One (1) Kodak SD 512 MB – 50110637L066

y. One (1) SanDisk Ultra II SD 1GB – B130631605228D

z. One (1) SanDisk MicroSD 128GB – 9093DVEXX0FO

aa. One (1) SanDisk MicroSD 128GB – 9531YXOHV1XA

bb. One (1) SanDisk MicroSD 128GB – 0023YXCYF2R2

cc. One (1) SanDisk MicroSD 128GB – 2123OC764584

dd. One (1) SanDisk MicroSD 256GB – 2093YCEKV14X

ee. One (1) SanDisk MicroSD 256GB – 8275DVCHQ06C

ff. One (1) SanDisk MicroSD 200GB – 8475DVKX80RY

gg. One (1) SanDisk MicroSD 32GB – 8166ZVAHR4X2

hh. One (1) SanDisk MicroSD 64GB – 8104DPLAK0QG

ii. One (1) Samsung Micro SD 128GB – DCQDH50GD636

jj. Two (2) Samsung Micro SD 128GB – DCQGX36GU635

kk. Two (2) Samsung Micro SD 128GB – DCQD1B1GK627

ll. One (1) Samsung Micro SD 128GB – DCQDK00GY635

mm. One (1) SanDisk Ultra USB 128GB – BP180726263B

nn. One (1) SanDisk Ultra USB 256GB – BQ180926263B

oo. One (1) SanDisk CruzerBlade 32 GB – BM70926126B

pp. One (1) SanDisk USB 32GB – BM170525476V

qq. One (1) Kingston Data Traveler 2GB – CH051008

rr. One (1) Blue USB – Entertainment Unlimited 8GB

ss. One (1) Orange USB Particle Measuring Systems

tt. One (1) San Disk SD Card 1GB – BB0814813316B

uu. One (1) Casio Exilim – 7125105A

vv. One (1) GoPro Hero 5, FCCID: CNFHWM91

This warrant authorizes the examination of the **TARGET DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records, in whatever format, on the **TARGET DEVICES**, as described in Attachment A, that relate to violations of Tile 18, United States Code, Section 2252(a) (Transport, Distribution, Receipt, and Possession of Child Pornography), and involve James WRIGHT, including:

a. records and information, in any format and medium, relating to the transportation, distribution, receipt, and possession of material depicting the sexual exploitation of a minor, to include the identity of any of the individuals involved;

b. records and information concerning communications, in any format or medium, relating to the transportation, distribution, receipt, and possession of material depicting the sexual exploitation of a minor or revealing a sexual interest in minors or the sexual exploitation of children, as well as the identity of any of the individuals involved;

c. records and information that reflect personal contact with other individuals to commit the referenced offenses, to include the identity of any of the individuals involved; and

d. in any format or medium, any originals, computer files, copies, and negatives of sexually exploitive imagery depicting minor(s), as defined in 18 U.S.C. § 2256(8) (child pornography); visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2); or any erotic, pornographic, or nude images/videos as they relate to the crimes under investigation.

2. Any notes, documents, records, or correspondence, in any format and medium (including e-mail messages, text messages, instant messages, chat logs, and other digital data files) pertaining to location information to commit the Target Offenses;

3. Any and all electronic address books, names, and lists of names and addresses of individuals on the **TARGET DEVICES** who James WRIGHT may have communicated with concerning the Target Offenses;

4. Any documents, records, or correspondence, pertaining to the ownership and use of the **TARGET DEVICES**, such as saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, text messages, photographs, and correspondence;

5. Evidence of user attribution showing who used or owned the **TARGET DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

6. Saved passwords, encryption keys, and other access devices that may be necessary to access information stored on the **TARGET DEVICES** or elsewhere. Any and all saved passwords and other data security devices designed to restrict access to, hide, or destroy software, documentation, or data. Data security devices may consist of software or other programming code. Any data which would reveal the presence of malware, viruses or malicious codes located on the computer storage media;

7. Evidence of the attachment to the **TARGET DEVICES** of other storage devices or similar containers for electronic evidence;

8. Records of, or information about, any of the **TARGET DEVICES**' internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or

"favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses;

9. Records evidencing the use of the Internet Protocol Addresses, including records of Internet Protocol Addresses used by the **TARGET DEVICES** and Internet Protocol Addresses used by computers that the **TARGET DEVICES** connected to;

10. Contextual information necessary to understand the evidence described in this Attachment.

In searching the **TARGET DEVICES**, law enforcement may examine all of the information contained in the **TARGET DEVICES** to view their precise contents and determine whether the **TARGET DEVICES** and/or information falls within the items to be seized, as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden," or encrypted information to determine whether the information falls within the list of items to be seized as set forth above.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any of the following:

a. Any form of computer or electronic storage (such as hard disks or other media that can store data);

b. Text messages or similar messages such as SMS or IM, saved messages, deleted messages, draft messages, call logs, all phone settings (*i.e.* call, messaging, display), priority senders, photographs, videos, links, account information, voicemails and all other voice recordings, contact and group lists, and favorites;

c. Pictures, all files, cloud files and relevant data without password access, storage information, documents, videos, programs, calendar information, notes, memos, word documents, PowerPoint documents, Excel Spreadsheets, and date and time data;

d. Payment information, to include account numbers, names, addresses, methods of payment, amounts, additional contact information, and financial institutions;

e. Lists and telephone numbers (including the number of the phone itself), names, nicknames, indicia of ownership and/or use, and/or other contact and/or identifying data of customer, co-conspirators, and financial institutions;

f. Applications (Apps), to include subscriber information, provider information, login information, contact and group lists, favorites, history, deleted items, saved items, downloads, logs, photographs, videos, links, messaging or other communications, or other identifying information;

g. Social media sites to include, name and provider information of social media network(s), profile name(s), addresses, contact and group lists (*i.e.* friends, associates, etc.), photographs, videos, links, favorites, likes, biographical information (*i.e.* date of birth) displayed on individual page(s), telephone numbers, email addresses, notes, memos, word documents, downloads, status, translations, shared information, GPS, mapping, and other information providing location and geographical data, blogs, posts, updates, messages, or emails;

h. Travel log records from GPS data (*i.e.* Google Maps and/or other Apps), recent history, favorites, saved locations and/or routes, settings, account information, calendar information, and dropped pinpoint information;

i. Internet service provider information, accounts, notifications, catalogs, Wi-Fi information, search history, bookmarks, favorites, recent tabs, deleted items and/or files,

downloads, purchase history, photographs, videos, links, calendar information, settings, home page information, shared history and/or information, printed history and/or information, or location data; and

j. Email data, including email addresses, IP addresses, DNS provider information, telecommunication service provider information, subscriber information, email provider information, logs, drafts, downloads, inbox mail, sent mail, outbox mail, trash mail, junk mail, contact lists, group lists, attachments and links, and any additional information indicative of the above-specified offenses.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts.